COMUNICADO DE SEGURIDAD CIBERNÉTICA

El CSIRT de Gobierno alerta ante resurgimiento de Remcos, malware difundido a través de archivos de Word

TLP: BLANCO

Como CSIRT de Gobierno hemos visto con mayor frecuencia, entre las campañas de phishing que detectamos, el uso del troyano **Remcos**, un peligroso virus informático que permite a un ciberdelincuente tomar total control del teléfono o computador de la víctima. También vemos que las campañas apuntan principalmente a empresas e instituciones públicas de nuestro país.

En vista de esta situación, y para ampliar el conocimiento de la ciudadanía respecto de las amenazas que enfrentamos en el ciberespacio, compartimos algunas de las características que hacen peligroso a Remcos, y algunas formas en que podemos evitar ser sus víctimas.

¿Por qué es tan riesgoso?

Este programa malicioso (un tipo de software también conocido como malware o virus) es difundido por ciberdelincuentes por medio de correos electrónico con la técnica de ***phishing***, esto es, emails maliciosos que se hacen pasar por un mensaje con el cual el receptor se sentirá confiado, interesado o presionado a abrir y ejecutar sus archivos adjuntos. Para lograrlo, en los mensajes de phishing se emplea un sinnúmero de mentiras, haciéndose pasar por mensajes laborales, de amistades o familiares, prometen premios o advierten de duras penas, como multas pendientes o la supuesta tenencia de contenido comprometedor del receptor del mensaje, por ejemplo.

Los delincuentes recurren a cualquier excusa con tal de que el receptor haga clic en un enlace o les envíe datos personales, como claves bancarias o códigos de recuperación de cuentas en redes sociales. Para mayor poder de convencimiento, Remcos va adjunto a estos emails disfrazado de tipos de archivo muy usados y conocidos en ambientes laborales, como .zip, .rar, .tar y .arj, o peor aún por lo común de su utilización, .docx, esto es, archivos del programa Word.

La estrategia más usada en ámbitos empresariales es adjuntar el malware Remcos como si fuera un archivo Word con una cotización, una factura u otro tipo similar de documento comercial, solicitando al receptor del mensaje que revise el documento para concretar un negocio.

Si se abre el archivo adjunto se descarga y ejecuta Remcos, lo que ocurre sin entregar ningún indicio al usuario. Remcos toma control total sobre el dispositivo infectando, permitiendo a los delincuentes desplegar programas conocidos como como keyloggers (que registran todo lo que se escribe desde el teclado, como usuarios y claves) y también softwares que guardan información del micrófono y toma capturas de pantallas.

¿Cómo protegerse de Remcos?: consejos para usuarios y para administradores de sistemas

Aprender a identificar y evitar los emails de phishing[1]: Debemos siempre estar atentos al recibir correos electrónicos o mensajes de texto, y evitar abrir o descargar adjuntos de cualquier mensaje sospechoso, es decir, principalmente emails que nos prometan alguna oferta increíble, que nos ganamos un premio o que tenemos una multa inesperada. Lo mismo con mensajes que nos pretenden alertar de problemas bancarios o bloqueos de tarjetas. Ante correos así, lo recomendable es contactar directamente al banco o institución para saber si la información recibida es real, en lugar de hacer clic en cualquier parte del correo sospechoso ni menos descargar algo que contenga.

Emplear programas de análisis del correo electrónico: Remcos se distribuye principalmente a través de email. El software de análisis de correo electrónico que identifica y bloquea mensajes sospechosos puede evitar que el malware llegue a las bandejas de entrada de los usuarios, por lo que las empresas e instituciones deben contar con este tipo de programas. A nivel de usuarios, el equivalente es usar programas de correo de proveedores confiables, como Gmail y Outlook, siempre recordando, eso sí, que ningún programa es infalible, y aplicando lo mencionado en el punto anterior.

Análisis de dominios: Remcos utiliza DDNS (Dynamic Domain Name System) para crear numerosos dominios de internet, con el fin de evadir el bloqueo de sitios maliciosos basado en dominios. El análisis de los registros de dominio solicitados por varios puntos finales puede ayudar a identificar nombres de dominio recientes y sospechosos, que podrían estar asociados con malware.

Análisis del tráfico de red: Algunas variantes de Remcos cifran directamente su tráfico de red utilizando AES-128[2] o RC4[3] en lugar de protocolos estándar como SSL/TLS[4]. El análisis del tráfico de red puede identificar estos flujos de tráfico inusuales y marcarlos para su posterior análisis.

Seguridad de puntos finales: Remcos es una variante de malware bien conocida con indicadores de compromiso establecidos. A pesar de sus técnicas de evasión de la defensa, las soluciones de seguridad para puntos finales pueden identificarlo y corregirlo en un sistema. Las 10 medidas esenciales que deberían tener en cuenta son:

- Antivirus y antimalware: Instalar y mantener actualizado un software antivirus y antimalware en los dispositivos finales para detectar y bloquear amenazas de malware y virus.

- Cortafuego personal: Utilizar un cortafuego personal en cada dispositivo final para controlar el tráfico de red y bloquear conexiones no autorizadas.

[1] https://www.csirt.gob.cl/recomendaciones/ciberguia-como-identificar-un-phishing/
[2] https://www.sciencedirect.com/topics/computer-science/advanced-encryption-standard
[3] https://www.geeksforgeeks.org/rc4-encryption-algorithm/. Es importante tener en cuenta que RC4 se considera actualmente un algoritmo de cifrado inseguro y se recomienda no utilizarlo. En su lugar, se deben utilizar algoritmos de cifrado modernos y más seguros como AES.
[4] https://www.cloudflare.com/learning/ssl/what-is-ssl-tls/

- Parches y actualizaciones: Mantener al día los sistemas operativos y aplicaciones en los puntos finales, aplicando parches y actualizaciones de seguridad para corregir vulnerabilidades conocidas.

- Autenticación y acceso seguro: Implementar autenticación fuerte, como contraseñas robustas, autenticación de dos factores o biométrica, para asegurar que solo usuarios autorizados puedan acceder a los puntos finales.

- Políticas de seguridad: Establecer políticas de seguridad claras que abarquen aspectos como el uso aceptable de los dispositivos finales, la prohibición de la instalación de software no autorizado y la protección de datos confidenciales.

- Control de dispositivos: Utilizar soluciones de gestión de dispositivos móviles (MDM) para controlar y asegurar los dispositivos móviles utilizados en la organización, como la capacidad de rastrear, bloquear o borrar datos de forma remota.

- Respaldo y recuperación: Implementar soluciones de respaldo y recuperación de datos en los puntos finales para garantizar la disponibilidad y restauración de información en caso de pérdida o daño.

- Monitoreo y detección de amenazas: Utilizar herramientas de monitoreo y detección de amenazas para identificar comportamientos anómalos o actividad maliciosa en los puntos finales y responder de manera oportuna.

- Educación y concienciación: Brindar formación y concienciación a los usuarios finales sobre las mejores prácticas de seguridad, como la identificación de correos electrónicos de phishing, la evitación de descargas de software no confiable y el uso seguro de contraseñas.

- Encriptación de datos: Utilizar técnicas de encriptación para proteger los datos almacenados en los dispositivos finales y en las comunicaciones entre los puntos finales y los servidores.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.18 17:11:14 -04'00'